

RISK MANAGEMENT POLICY

Type	Governance
Category	Corporate & Community
Responsible Officer	Director Corporate & Community
First Issued / Adopted	28 January 2009
Review Period	4 Years
Last Reviewed	22 October 2025, 26 July 2023, 22 January 2020, 22 March 2017
Reference	OM259/25, OM309/23, OM14/20, OM84/17
Next Review Date	November 2029
Applicable Legislation	Civil Liabilities Act 1936 Local Government Act 1999 (refer Appendix B). WHS Act 2012
Related Documents	AS/NZS ISO31000:2018 Risk Management – Guidelines (supersedes AS/NZS ISO31000:2009) Code of Conduct for Self-Insured Employers (2016) LGRS Risk Management Framework (Feb 2024) LGRS Risk Management Policy (Feb 2024) Risk Management Framework (PPRC) Enterprise Risk Management Procedure (PPRC) Enterprise Risk Register (Strategic & Operational) Work Health, Safety & Return to Work Policy (PPRC)
Public Consultation Required	No
File Reference (Altus)	2024. 1319 working copies 2025.0852 MASTER document

1. PURPOSE

Port Pirie Regional Council (Council) recognises that effective risk management improves decision-making, prioritises resources, protects people and assets, and supports delivery of our vision and strategic objectives.

This Policy aims to enable an integrated, consistent and systematic approach to risk management by :

- a) Stating Council's commitment to core risk management principles (AS ISO 31000:2018);
- b) Detailing roles and responsibilities for risk governance and oversight ;
- c) Supporting implementation and continual improvement of Council's Risk Management Framework (the Framework), procedures and tools; and
- d) Ensuring regular review, assurance and reporting on strategic, financial and operational risks and controls.

Risk management is an essential component of good governance and public accountability.

2. SCOPE

The policy applies to Elected Members, members of Council Committees, employees, volunteers, contractors and consultants and to all activities, decisions and services undertaken by or on behalf of Council.

3. DEFINITIONS

See **Appendix A**.

4. POLICY

4.1 Commitment & Principles

Risk management will be integrated into Council's governance, leadership, strategy, planning, budgeting, projects, procurement, contracts and service delivery. Council adopts the principles of AS ISO 31000:2018: integrated; structured & comprehensive; customized; inclusive; dynamic; uses best available information; considers human & cultural factors; and drives continual improvement.

4.2 Risk Governance & Framework

Council will maintain a Risk Management Framework that sets out processes, tools and criteria for:

- a) Communication & consultation
- b) Scope, context & risk criteria (including risk appetite & tolerance)
- c) Risk identification, analysis, evaluation & treatment
- d) Recording & reporting (including registers and dashboards)
- e) Monitoring, review & assurance (including internal audit alignment)
- f) Continuous improvement and maturity assessment

The Framework will align to AS ISO 31000:2018 and the LGRS Risk Management Framework (Feb 2024).

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 2 of 9

4.3 Risk Appetite & Tolerance

Council will set and periodically review a Risk Appetite Statement (within the Framework), expressing the types and levels of risk it is willing to accept in pursuit of objectives. Risk tolerance thresholds will guide escalation and treatment priorities.

4.4 Roles & Responsibilities

a) Council

- (i) Sets the risk appetite and approves this Policy and the Framework.;
- (ii) Considers risk information when setting strategy and making decisions;
- (iii) Ensures appropriate risk governance structures (including the Audit & Risk Management Committee (ARMC)) and delegations are in place; and
- (iv) Requires the CEO to demonstrate effectiveness of risk management and provide visibility of material risks impacting objectives.

b) Audit and Risk Management Committee (ARMC)

- (i) Provides oversight of risk management and internal audit planning;
- (ii) Reviews the adequacy and effectiveness of the Framework and related policies, systems and procedures; and
- (iii) Reviews risk reports (including top strategic risks, treatments and control assurance) at least annually and recommends improvements to Council.

c) Chief Executive Officer (CEO)

- (i) Champions a risk-aware culture and clear accountability;
- (ii) Ensures the Framework is implemented across all activities;
- (iii) Ensures effective policies, systems and processes for identifying, assessing, treating, monitoring and reporting risks;
- (iv) Allocates ownership for risks and treatments; ensures capability of the EMT and managers;
- (v) Provides regular reports to ARMC and Council on risks, treatment progress, and internal audit outcomes; and
- (vi) Escalates risks exceeding appetite to ARMC/Council as required.

d) Executive Management Team (EMT)

- (i) Leads and embeds risk management in their portfolios and decisions;
- (ii) Maintains the Enterprise Risk Register (strategic & operational) with regular reviews and updates;
- (iii) Ensures timely implementation and close-out of risk treatments and internal audit actions; and
- (iv) Reviews emerging risks and key risk indicators (KRIs) and ensures integration with business planning, projects and procurement.

e) Governance & Risk Coordinator (Strategic Risk Management)

- (i) Maintains the Framework and Enterprise Risk Register, ensuring consistency and currency;
- (ii) Coordinates reporting on the risk profile, treatments and control assurance;
- (iii) Facilitates risk assessment workshops, training and maturity reviews; and
- (iv) Aligns risk activities with internal audit and the LGRS program.

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 3 of 9

f) Employees, Volunteers and Contractors

- (i) Identify, assess, manage and/or escalate risks in their work and projects.
- (ii) Apply the Framework and procedures; implement assigned controls and treatments.
- (iii) Report incidents, hazards and control failures promptly and participate in reviews and training.

4.5 Risk Management Process (AS ISO 31000:2018)

Council will apply the following lifecycle across activities and projects:

- a) Communication & Consultation with stakeholders;
- b) Scope, Context & Criteria (including appetite/tolerance, consequence & likelihood tables);
- c) Risk Identification (strategic, operational, project, financial, compliance, fraud & corruption, WHS, cyber, climate, supplier/contractor, asset & infrastructure, reputation);
- d) Risk Analysis (causes, existing controls, consequence/likelihood, inherent vs residual risk);
- e) Risk Evaluation (compare to appetite/tolerance; prioritise);
- f) Risk Treatment (avoid, reduce, transfer/share, accept with rationale); assign owners, actions, due dates and KRIs;
- g) Recording & Reporting (registers, dashboards, ARMC/Council reports);
- h) Monitoring & Review (control effectiveness, treatment progress, incidents & near misses, KRI thresholds);
- i) Continuous Improvement (lessons learned, audit outcomes, maturity assessments).

4.6 Integration with Planning, Projects & Procurement

- a) Risk analysis will inform strategic planning, annual business planning and budgeting;
- b) Section 48 (LG Act) prudential and major project decisions will include documented risk analysis and treatments;
- c) Procurement and contract management will include supplier risk assessment, safety and insurance requirements, and performance monitoring; and
- d) Business Continuity and Emergency Management arrangements will be maintained and exercised, with interdependencies recorded in the risk register as appropriate.

4.7 Performance Measures

Council will monitor and report on the effectiveness of risk management using indicators such as:

- a) % of strategic & operational risks reviewed on schedule
- b) Reduction in number/percentage of Extreme/High residual risks

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 4 of 9

- c) % of risk treatments on track/closed by due date
- d) % of audit actions closed by due date
- e) Training coverage: % of Elected Members, managers and staff trained
- f) KRI threshold breaches detected, escalated and resolved within target timeframes
- g) Progressive improvement in risk maturity (periodic assessment)

4.8 Legislative & Scheme Context

- a) Legislative obligations under the Local Government Act 1999 (see Appendix B) require Councils to identify, manage and report on risks, maintain internal control, and ensure effective internal audit oversight.
- b) As a member of the LGA Mutual Liability Scheme (LGRS), Council will implement adequate risk prevention strategies to minimise incidents and claims and will align to the LGRS Risk Management Framework (Feb 2024).

5. DOCUMENT REVIEW

This Policy will be reviewed every four years, or earlier if required by changes in legislation, related documents, WHS requirements, Council intent, delegated authorities, or by CEO/Director determination.

6. FURTHER INFORMATION

This policy is available for inspection at:

- a) Port Pirie Regional Council Principal Administration Office, 115 Ellen St. Port Pirie;
- b) Crystal Brook Office, 21 Bowman Street, Crystal Brook.

It can be downloaded, free of charge, from Council's internet site: www.pirie.sa.gov.au

Copies are available on request (fees may apply in line with Council's Schedule of Fees and Charges).

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 5 of 9

7. DOCUMENT HISTORY

Version No.	Date Approved	Minute Reference	Notes/ changes
V1.0	28/01/2009		New document
	22/03/2017	OM84/17	Review (details not recorded)
	22/01/2020	OM14/20	Review (details not recorded)
V2.0	26/07/2023	OM309/23	<p><u>Added:</u> Civil Liabilities Act and AS/NZS ISO31000:2018 Risk Management Guidelines.</p> <p><u>Updated:</u> Audit Committee to Audit & Risk Management Committee (Sect. 5.2); formatting.</p> <p><u>Deleted:</u> location of Council Administration Offices and directed members of the public to Council website (Sect 6. Further Information).</p>
V3.0	22/10/2025	OM259/25	<p>Full redraft: aligned to AS ISO 31000:2018 and LGRS 2024; clarified roles & reporting; introduced appetite/tolerance; integrated with planning, projects & procurement; strengthened KPIs;</p> <p>Added: Appendices A–B. from Risk Management Framework document and refreshed.</p>

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 6 of 9

APPENDIX A – Definitions APPENDIX A – Definitions**Assurance**

A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk

Consequence

An outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

Control

An action that modifies and increases the likelihood that the objectives and goals of the organisation will be achieved

Enterprise Risk Management

The process that is applied in strategy setting and decision making throughout the organisation to identify, evaluate and manage potential risks that are likely to impact on achievement of objectives, set risk appetite and tolerance and manage risk within those parameters, and to provide reasonable assurance regarding the achievement of the organisation's objectives.

Establishing the Context

Defining the external and internal parameters to be taken when managing risk

Event

The occurrence of a particular set of circumstances

Exposure/ Rating

The risk exposure (also referred to as risk rating) which is a qualitative value of the sum of the consequence of an event multiplied by the likelihood of that event occurring

External Context

The external environment in which the organisation seeks to achieve its objectives

Frequency

Measure of the rate of occurrence of an event expressed as the number of occurrences of the event in a given time

Internal audit

Independent objective assurance activity that uses a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes

Internal Context

The internal environment in which the organisation seeks to achieve its objectives

Likelihood

The chance of something happening

Monitor

To check, supervise, observe critically or record the progress of an activity, action or system on a regular basis in order to identify change.

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 7 of 9

Reasonable assurance

The concept that enterprise risk management, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of inherent limitations in all Risk Management Frameworks.

Residual Risk

A risk remaining after risk treatment.

Risk

The effect of uncertainty on objectives.

Risk Analysis

The systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk Appetite

An amount and type of risk that Council is prepared to accept in pursuit of its objectives.

Risk Assessment

An overall process of risk identification, risk analysis and risk evaluation.

Risk Culture

The behavioural standards that lead to how every person thinks about and manages risk.

Risk Evaluation

means the process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.

Risk Management

means the Coordinated activities to direct and control an organisation with regard to risk.

Risk Management Framework

A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk Owner

An employee with the accountability and authority to manage a risk.

Risk Rating

A Risk priority based on consequence and likelihood assessments.

Risk Register

A Register of all identified risks, their consequences, likelihood, rating and treatments.

Risk Tolerance:

The acceptable variation in outcomes related to specific performances measures linked to objectives the organisation seeks to achieve.

Stakeholder

A person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity.

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 8 of 9

Appendix B – Legislative Requirement

Section of Local Government Act	Legislative requirement
48	Requires Council to: identify risks associated with a project and take steps to manage, reduce or eliminate those risks, (including by provision of periodic reports to the CEO and to the Council.
99 (1)(ia)	Requires the CEO to: ensure that effective policies, systems and processes are established and maintained for the identification, assessment, monitoring, management and annual review of strategic, financial and operational risks.
125	Requires Council to: ensure that appropriate policies, practices and procedures of internal control are implemented and maintained in order to assist the organisation to carry out its activities in an efficient and orderly manner to achieve its objectives.
125 A	Requires the person primarily responsible for the internal audit function to: ensure that any reports they prepare relating to the internal audit function are provided directly to the Audit and Risk Management Committee and may report any matters relating to the internal audit function directly to the Audit and Risk Committee.
126 126 A(4)(g)	Requires the council Audit and Risk Management Committee to: provide oversight of planning and scoping of the internal audit work plan and to review and comment on reports provided by the person primarily responsible for the internal audit function at least on a quarterly basis; and Review and comment on an annual report provided by the CEO in relation to the policies and processes adopted by the council to evaluate and improve the effectiveness of its internal control practices and procedures.
126 A(4)(h)	Requires the council Audit and Risk Management Committee to: review and evaluate the effectiveness of policies, systems and procedures established and maintained for the identification, assessment, monitoring, management and review of strategic, financial and operational risks on a regular basis.
132 A	Requires Council to: ensure that appropriate policies, practices and procedures are implemented and maintained in order to ensure compliance with statutory requirements and achieve and maintain standards of good public administration.
134 (4)(b)	Requires Council to: adopt risk management policies, controls and systems by a resolution passed by at least a two thirds majority of the Elected Members prior to entering into financial arrangements for the purpose of managing, hedging or protecting against interest rates or other costs of borrowing money.

Document No	Version No	Last review	Next review	Page
POL-0006	3.0	22/10/2025	November 2029	Page 9 of 9